两类低重二元线性码的重量分布和重量谱

李斐

(安徽财经大学 统计与应用数学学院，安徽 蚌埠 233030)

摘　要： 构造线性码是编码密码理论中的重要研究课题. 码的重量分布和重量谱的决定在编码理论中也有着基本的理论意义，而且在保密通信中有重要作用. 本文构造了一类3-重和一类4-重二元线性码，并完全确定了它们的重量分布和重量谱.

关　键　词： 线性码；重量分布；重量谱；广义汉明重量

中图分类号： TN911.22　**文献标志码：** A　　**文章编号：** 1008-9497(0000)00-000-00

Two families of binary linear codes and their weight distributions and weight hierarchies Journal of Zhejiang University (Science Edition)，2023, 00

Abstract: Constructing linear codes with few weights is an important research topic in coding and cryptography theory. The weight hierarchy of code also has basic theoretical significance in coding theory, and plays an important role in secret communications. In this paper, a class of 3-weight and a class of 4-weight binary linear codes are constructed, and their weight distributions and weight hierarchies are determined by exponential sum theory.

Key Words: linear code; weight distribution; weight hierarchy; generalized Hamming weight

1 引言和主要结果

本文中，p 表示一个素数，s 表示一个正整数，F_{p^s} 表示一个含有 p^s 个元素的有限域，$F_{p^s}^*$ 表示该有限域的乘法群.

如果 C 是 F_p^n 的一个 k 维子空间，而且 C 的不同元素之间最小汉明距离为 d，我们称之为参数[n ,k,d]的线性码. 对于 $i\in\{1, 2, \dots, n\}$，我们用 A_i 表示线性码 C 中汉明重量等于 i 码字的个数. 序列$(1,A_1,\dots,A_n)$，我们称之为线性码 C 的重量分布. 如果序列 $(A_1,\dots,A_n)$中不等于零的数字个数为 t，我们就称线性码 C 为一个 t-重码. 线性码的重量分布是编码理论中的经典研究课题，备受关注. 对于一个 t-重码，如果 t 较小，我们称该码为低重码. 低重的线性码在认证码[11]，结合方案[6]，秘密共享方案[39]，和强正则图[7]等方面有很多重要实际用途和理论应用.

在上世纪 70 年代，受到密码应用的推动，人们引入了线性码的广义汉明重量的概念[13,18]. 令$[C,r]_p$表示 C 的所有 r 维 F_p 上的子空间的集合. 对于$[C,r]_p$中的一个子空间 V，我们定义 Supp(V) $=\{i:1\le i\le n, c_i\neq 0$ 对于某个 $c=(c_1, c_2, \dots, c_n)\in V\}$.

收稿日期： 2022-00-00.

基金项目： 安徽省自然科学基金面上项目(1908085MA02).

作者简介： 李斐(1977-)，ORCID:https://orcid.org/0000-0001-7394-5273，男，副教授，博士，主要从事代数编码和代数数论研究，E-mail:cczxlf@163.com.

定义 1 令 C 为一个 F_p 上的$[n, k, d]$线性码. 对于 $1 \le r \le k$, 定义

$$d_r(C)=\min\{|Supp(V)|:V \in [C,r]_p\}.$$

则称 $d_r(C)$ 为 C 的第 r 个广义汉明重量(Generalized Hamming weight，简记为 GHW). 同时，序列$\{d_r(C) : 1 \le r \le k\}$ 称为 C 的重量谱 (Weight hierarchy).

易见，$d = d_1(C)$. 广义汉明重量可视为最小汉明重量概念的推广. 当线性码用于和密码系统相连的 II 型的窃听信道时，重量谱可以完全刻画线性码的运作模式. 同时，重量谱在码的格子复杂度分析等方面有重要应用[14,36,37]. 尤其，自从学者 Wei 于 1991 发表经典论文[37]以后，人们对它的兴趣越来越高. 在 1996 年，陈文德和挪威学者 T. Klϕve 合作，首次提出有限射影几何的方法研究重量谱，取得了丰富的成果[5]. 关于代数几何码，BCH 码，Reed-Muller 码，循环码这几类线性码，对它们的重量谱已知道很多[1,4,15,17,38,40]. 近来，出现了一些线性码的重量谱的结果[40,3,28].

香港科技大学丁存生教授等给出了一个构造线性码的一般性方法[10]，如下：令 Tr 表示从 F_{p^s} 到 F_p 的迹函数，D= $\{d_1,d_2,\dots,d_n\}$ 为 $F_{p^s}^*$ 的一个子集. 一个长度为 n 的线性码定义为:

$$C_D=\{(Tr(xd_1),Tr(xd_2),\dots,Tr(xd_n)): x \in F_{p^s}^*\}, \quad (1)$$

其中，D 被称为线性码 C_D 的定义集. 通过选择合适的定义集，人们构造出了一些低重的最优线性码[8,9,12,19-21,35,41,42].

安徽大学施敏加等学者对该法做了改进，在有限域的扩环上构造出许多低重的最优码和极小码，其中大部分也可以用于构建秘密共享方案(见参考文献[2,30-34]).

在文献 [23,24] 中，华东师范大学的李成举等学者对定义集构造线性码方法进行了一般化，构造出低重线性码. 这个一般化的方法如下：

设 e 为一个正整数，$D=\{d_1,d_2,\dots,d_n\}$ 为 $F_{p^s}^e\setminus\{(0,0,\dots,0)\}$的一个子集. 对于 $F_{p^s}^e$ 中的两个向量 $u=(u_1,u_2,\dots,u_e)$, $v=(v_1,v_2,\dots,v_e)$ ，令 $u \bullet v$ 表示它们的内积，即 $u \bullet v=u_1v_1+u_2v_2+\dots+u_ev_e$.

一般地，定义一个长度为 n 线性码 C_D 如下：

$$C_D=\{(Tr(x \bullet d_1),Tr(x \bullet d_2),\dots,Tr(x \bullet d_n)): x \in F_{p^s}^e\}. \quad (2)$$

这里 D 仍称之为定义集. 应用该法和选择适当的定义集，一些低重线性码被构造出来[2,16].

本文在这里和之后作如下设定：设 ρ 为一个素数，且 2 是模 ρ^m 的一个本原根. 同时，令 ϕ 为数论欧拉函数，即有 $\phi(\rho^m)=\rho^{m-1}(\rho-1)$.

我们取定 p=2, $q=2^{\phi(\rho^m)}$.

本文中，我们构造线性码的定义集 $D=\{d_1,d_2,\dots,d_n\}$选择如下： $a \in F_{p^s}^*, b \in F_{p^s}$，令

$$D=D(a,b)=\{(x,y) \in F_{p^s}^2 \setminus\{(0,0)\}: Tr(a x^{\frac{q-1}{\rho^m}} + by)=1\}.$$

因此，线性码 $C_{D(a,b)}$构造如下:

$$C_{D(a,b)}=\{(Tr(x \bullet d_1),Tr(x \bullet d_2),\dots,Tr(x \bullet d_n)):x \in F_{p^s}^2\}. \quad (3)$$

利用[27]中的方法，我们构造了新的两类低重量二元线性码，解决了它们的重量分布和重量谱. 我们的主要结果为如下定理 2-5:

定理 2 设 $a \in F_{p^s}^*$. 如(3)所定义的线性码 $C_{D(a,0)}$，它是以$[n, 2\phi(\rho^m), d]$为参数的二元码，其中 $n=\frac{q}{2}(q-1-\frac{(q-1)S(a)}{\rho^m})$, $d=\frac{q}{4}(q-\sqrt{q}-\frac{(q+\sqrt{q})S(a)}{\rho^m})$. 其重量分布见表 1.

表 1 定理 2 中线性码的重量分布

重量	频数
0	1
$\frac{q}{4}(q-1)(1-\frac{S(a)}{\rho^m})$	$q(q-1)$
$\frac{q}{4}(q+\sqrt{q}-\frac{(q+\sqrt{q})S(a)}{\rho^m})$	$\frac{1}{2}(q-1)(1+\frac{S(a)}{\rho^m})$
$\frac{q}{4}(q-\sqrt{q}-\frac{(q+\sqrt{q})S(a)}{\rho^m})$	$\frac{1}{2}(q-1)(1-\frac{S(a)}{\rho^m})$

定理 3 设 a，$b \in F_{p^s}^*$. 如(3)所定义的线性码 $C_{D(a,b)}$，它是以$[\frac{1}{2}q^2, 2\phi(\rho^m)]$为参数的二元码，

它的重量分布见表 2.

表 2 定理 3 中线性码的重量分布

重量	频数
0	1
$\frac{q}{4}(q+1+\frac{(q-1)S(a)}{\rho^m})$	1
$\frac{q}{4}(q+1-\sqrt{q}-\frac{(1+\sqrt{q})S(a)}{\rho^m})$	$\frac{1}{2}(q-1)(1+\frac{S(a)}{\rho^m})$
$\frac{q}{4}(q+1+\sqrt{q}-\frac{(1+\sqrt{q})S(a)}{\rho^m})$	$\frac{1}{2}(q-1)(1-\frac{S(a)}{\rho^m})$
$\frac{1}{4}q^2$	q^2-q-1

定理 4 设 $a\in F_{p^s}^*$. 如(3)所定义的线性码 $C_{D(a,0)}$，它的重量谱为

$$d_r(C_{D(a,0)})=\begin{cases}\frac{1}{2}q(1-2^{-r})(q-\sqrt{q}-\frac{(q+\sqrt{q})S(a)}{\rho^m}), 1\le r\le\frac{1}{2}\phi(\rho^m)\\ \frac{1}{2}q(q-1-\frac{(q-1)S(a)}{\rho^m})+1-\frac{q^2}{2^r}, \frac{1}{2}\phi(\rho^m)<r\le 2\phi(\rho^m).\end{cases}$$

定理 5 设 a，$b\in F_{p^s}^*$. 如(3)所定义的线性码 $C_{D(a,b)}$，它的重量谱为

(1) 当 $1\le r\le\frac{1}{2}\phi(\rho^m)$，$S(a)<0$，则有

$$d_r(C_{D(a,b)})=\frac{1}{2}q^2(1-\frac{1}{2^r})+\frac{q}{4}(1-\frac{(\sqrt{q}+1)S(a)}{\rho^m}-\sqrt{q})+\frac{q\sqrt{q}}{2^{r+1}}(1+\frac{(\sqrt{q}+1)S(a)}{\rho^m})$$

(2) 当 $1\le r\le\frac{1}{2}\phi(\rho^m)$，$S(a)>0$，则有

$$d_r(C_{D(a,b)})=\frac{1}{2}q^2(1-\frac{1}{2^r})+\frac{q}{4}(1-\frac{(\sqrt{q}+1)S(a)}{\rho^m}-\sqrt{q})$$

(3) 当 $\frac{1}{2}\phi(\rho^m)<r\le 2\phi(\rho^m)$，则有

$$d_r(C_{D(a,b)})=\frac{1}{2}q^2(1-2^{1-r})+1\cdot$$

2 预备知识和结论

2.1 一个计算 $d_r(C_D)$ 的公式

对于(2)所定义的线性码 C_D，文献[27]给出了一个计算广义汉明重量的 $d_r(C_D)$ 的公式，见如下引理.

引理 1 ([27]，Proposition 1) 对于 $1\le r\le es$，如果线性码 C_D 的维数为 es，那么

$$d_r(C_D)=n-\max\{|D\cap H|: H\in[F_{p^s}^e, es-r]_p\}.$$

2.2 一个指数和

回顾一下在前面我们设定了 $p=2$，$q=2^{\phi(\rho^m)}$. 令 γ 为 F_q^* 的一个固定的本原元，设 $\alpha=\gamma^{\frac{q-1}{\rho^m}}$. 令 χ_1 为 F_q 上的典范加法特征，即 $\chi_1(x)=(-1)^{Tr(x)}$. 关于有限域上的加法特征更多信息，读者可参考文献[22].

对于 $a,b\in F_q$，有两个如下定义的指数和：

$$S(a)=\sum_{i=0}^{\rho^m-1}\chi_1(a\alpha^i) \quad 和 \quad S(a, b)=\sum_{x\in F_q^*}\chi_1(ax^{\frac{q-1}{\rho^m}}+bx)\cdot$$

因为 2 是模 ρ^m 的本原根，故有 $F_q=F_2(\alpha)$. 因此 $\{\alpha^1,\alpha^2,\cdots,\alpha^{\phi(\rho^m)}\}$ 是 F_q 作为 F_2 上线性空间的一个基.那么对于 F_q 中的一个元素 u 可以表示如下：

$$u=\sum_{j=1}^{\phi(\rho^m)}a_j\alpha^j, a_j\in F_2.$$

对于 $i=0,1,\cdots,\rho^{m-1}-1$，令 $u^{(i)}$ 为 u 在该基下的坐标向量 $u=(a_1,a_2,\cdots,a_{\phi(\rho^m)})$ 的一个长度为 $\rho-1$ 的子向量，具体如下：

$$u^{(i)}=(a_{\rho^{m-1}-i},a_{2\rho^{m-1}-i},\cdots,a_{(\rho-1)\rho^{m-1}-i}).$$

令 wt(x) 为向量 x 的汉明重量. 对于 $a\in F_q^*$，定义 F_q 的两个子集，如下：

$$E_a=\{u\in F_q^*: wt((au^{\frac{q-1}{\rho^m}})^{(0)})为偶数\}$$

$O_a=\{u\in F_q^*: wt((au^{-\frac{q-1}{\rho^m}})^{(0)})为奇数\}$.

关于上面两个指数和及 E_a，O_a，有下面几个重要引理：

引理 2 ([29]，Theorem 1) 令 $a\in F_q$，则有

$$S(a)=\sum_{i=0}^{\rho^{m-1}-1}(-1)^{wt(a^{(i)})}(\rho-2wt(a^{(i)})).$$

引理 3 ([29]，Theorem 3) 当 a 跑遍 F_q^* 的所有值，S(a) 的所有取值为集合

$$\{\rho^m-4j: j=1,2,\cdots,\frac{1}{2}\phi(\rho^m)\}.$$

引理 4 ([20]，Lemma 4) 令 $a\in F_q^*$，$b\in F_q$. 当 $b\neq 0$，令 $c=ab^{-\frac{q-1}{\rho^m}}$. 那么有

$$S(a，b)=\begin{cases}\frac{q-1}{\rho^m}S(a)，当b=0,\\(-1)^{wt(c^{(0)})}\sqrt{q}-\frac{\sqrt{q}+1}{\rho^m}S(a)，当b\neq 0.\end{cases}$$

引理 5 ([27]，Corollary 1) 对于任意 $a\in F_q^*$，有

$$|E_a|=\frac{1}{2}(q-1)(1+\frac{S(a)}{\rho^m})，|O_a|=\frac{1}{2}(q-1)(1-\frac{S(a)}{\rho^m}).$$

3 主要定理的证明

首先我们来计算线性码 $C_{D(a,b)}$ 的长度 n，见如下引理.

引理 6 对于任意 $a\in F_q^*$，$b\in F_q$，那么有

$$n=|D(a,b)|=\begin{cases}\frac{q}{2}(q-1-S(a,0))，当b=0,\\\frac{q^2}{2}，当b\neq 0.\end{cases}$$

证明 利用加法特征的正交性，我们有

$$|D(a,b)|=\frac{1}{2}\sum_{x,y\in F_q}(1+\chi_1(ax^{\frac{q-1}{\rho^m}}+by-1))$$

$$=\frac{1}{2}q^2-\sum_{y\in F_q}\chi_1(by)\sum_{x\in F_q}\chi_1(ax^{\frac{q-1}{\rho^m}}).$$

当 $b=0$，易见 $|D(a,0)|=\frac{q}{2}(q-1-S(a,0))$. 当 $b\neq 0$，由于 $\sum_{y\in F_q}\chi_1(by)=0$，易见 $|D(a,b)|=\frac{1}{2}q^2$.

证明结束.

3.1 定理 2 和定理 3 的证明

设 $(u,v)\in F_q^2$，令 $c_{(u,v)}$ 为 $C_{D(a,b)}$ 中与其对应的码字，即

$$c_{(u,v)}=(Tr(ux+vy))_{(x,y)\in D(a,b)}.$$

易见 $c_{(0,0)}=0$，且 $wt(c_{(0,0)})=0$. 因此假设 $(u,v)\neq(0,0)$，在下面的引理中我们给出了码字 $c_{(u,v)}$ 的汉明重量 $wt(c_{(u,v)})=0$.

引理 7 设 $(u,v)(\neq(0,0))\in F_q^2$，则有

(1) 如果 $b=0$，则有

$$wt(c_{(u,v)})=\begin{cases}\frac{q}{4}(q-1-S(a,0))，当v\neq 0,\\\frac{q}{4}(q-S(a,0)+S(a,u))，当v=0.\end{cases}$$

(2) 如果 $b\neq 0$，则有

$$wt(c_{(u,v)})=\begin{cases}\frac{q^2}{4}，当v\neq b,\\\frac{q}{4}(q+1+S(a,u))，当v=b.\end{cases}$$

证明 令 $N(u,v)=$

$$\{(x,y)\in F_q^2: Tr(ax^{\frac{q-1}{\rho^m}}+by)=1，Tr(ux+vy)=0\},$$

那么 $N(u,v)=$

$$\frac{1}{4}\sum_{x,y\in F_q}(\sum_{z\in F_2}\chi_1(z(ax^{\frac{q-1}{\rho^m}}+by-1))\sum_{w\in F_2}\chi_1(w(ux+vy)))$$

$$=\frac{1}{4}\sum_{x,y\in F_q}((1-\chi_1(ax^{\frac{q-1}{\rho^m}}+by))(1+\chi_1(ux+vy)))$$

$$=\frac{q^2}{4}-\frac{1}{4}\sum_{x,y\in F_q}\chi_1(ax^{\frac{q-1}{\rho^m}}+by)-$$

$$\frac{1}{4}\sum_{x,y\in \mathrm{F_q}}\chi_1(\mathrm{a}x^{\frac{\mathrm{q}-1}{\rho^{\mathrm{m}}}}+ux+vy+\mathrm{b}y).$$

下面我们对 $\mathrm{b}=0$ 和 $\mathrm{b}\neq 0$ 这两种情形分别给以证明.

(1) 如果 $\mathrm{b}=0$，则有 $|N(u,v)|=$

$$\frac{1}{4}(\mathrm{q}^2-\mathrm{q}(1+\mathrm{S(a,0)})-(1+\mathrm{S}(\mathrm{a},u))\sum_{y\in \mathrm{F_q}}\chi_1(vy)).$$

因此有

$$|N(u,v)|=\begin{cases}\frac{\mathrm{q}}{4}(\mathrm{q}-1-\mathrm{S(a,0)}), & 当 v\neq 0,\\ \frac{\mathrm{q}}{4}(\mathrm{q}-2-\mathrm{S(a,0)}-\mathrm{S}(\mathrm{a},u)), & 当 v=0.\end{cases}$$

由 $\mathrm{wt}(c_{(u,v)})=n-|N(u,v)|$ 和引理 6，则得证.

(2) 如果 $\mathrm{b}\neq 0$，则有 $|N(u,v)|$

$$=\frac{\mathrm{q}^2}{4}-\frac{1}{4}\sum_{x,y\in \mathrm{F_q}}\chi_1(\mathrm{a}x^{\frac{\mathrm{q}-1}{\rho^{\mathrm{m}}}}+ux+vy+\mathrm{b}y)$$

$$=\frac{\mathrm{q}^2}{4}-\frac{1}{4}(1+\mathrm{S}(\mathrm{a},u))\sum_{y\in \mathrm{F_q}}\chi_1(vy+\mathrm{b}y).$$

因此有 $|N(u,v)|=\begin{cases}\frac{\mathrm{q}^2}{4}, & 当 v\neq \mathrm{b},\\ \frac{\mathrm{q}}{4}(\mathrm{q}-1-\mathrm{S}(\mathrm{a},u)), & 当 v=\mathrm{b}.\end{cases}$

同样利用引理 6，我们可得证. 证明结束.

下面我们给出**定理 2** 的证明:

设 $(u,v)\neq(0,0)$，由引理 7 可知 $\mathrm{wt}(c_{(u,v)})>0$. 因此映射 $\mathrm{F_q^2}\to \mathrm{C_{D(a,0)}}$：$(u,v)\to c_{(u,v)}$ 是线性空间的同构映射. 故线性码 $\mathrm{C_{D(a,0)}}$ 的维数为 $2\phi(\rho^{\mathrm{m}})$. 由引理 7 和引理 4 可知 $\mathrm{wt}(c_{(u,v)})$ 可取 3 个值，它们是

$$\begin{cases}\omega_1=\frac{\mathrm{q}}{4}(\mathrm{q}-1-\frac{(\mathrm{q}-1)\mathrm{S(a)}}{\rho^{\mathrm{m}}}),\\ \omega_2=\frac{\mathrm{q}}{4}(\mathrm{q}-\sqrt{\mathrm{q}}-\frac{(\mathrm{q}+\sqrt{\mathrm{q}})\mathrm{S(a)}}{\rho^{\mathrm{m}}}),\\ \omega_3=\frac{\mathrm{q}}{4}(\mathrm{q}-\sqrt{\mathrm{q}}-\frac{(\mathrm{q}+\sqrt{\mathrm{q}})\mathrm{S(a)}}{\rho^{\mathrm{m}}}).\end{cases}$$

由引理 7 中 $|N(u,v)|$ 的计算和引理 5，我们可得线性码 $\mathrm{C_{D(a,0)}}$ 的重量分布，见表 1 所示. 证明结束.

下面我们给出**定理 3** 的证明:

据引理 6 可知线性码 $\mathrm{C_{D(a,b)}}$ 的长度. 同理定理 2 的证明，可知该线性码的维数也是 $2\phi(\rho^{\mathrm{m}})$. 对于 $(u,v)\neq(0,0)$，由引理 7 和引理 4 可知 $\mathrm{wt}(c_{(u,v)})$ 有 4 个取值，如下

$$\begin{cases}\omega_1=\frac{\mathrm{q}}{4}(\mathrm{q}+1+\frac{(\mathrm{q}-1)\mathrm{S(a)}}{\rho^{\mathrm{m}}}),\\ \omega_2=\frac{\mathrm{q}}{4}(\mathrm{q}+1-\sqrt{\mathrm{q}}-\frac{(1+\sqrt{\mathrm{q}})\mathrm{S(a)}}{\rho^{\mathrm{m}}}),\\ \omega_3=\frac{\mathrm{q}}{4}(\mathrm{q}+1+\sqrt{\mathrm{q}}-\frac{(1+\sqrt{\mathrm{q}})\mathrm{S(a)}}{\rho^{\mathrm{m}}}),\\ \omega_4=\frac{\mathrm{q}^2}{4}.\end{cases}$$

由引理 7 中 $|N(u,v)|$ 的计算和引理 5 可知重量为 ω_i 的码字个数 A_{ω_i} 的取值. 因此我们得到 2 中线性码 $\mathrm{C_{D(a,b)}}$ 的重量分布. 证明结束.

3.2 定理 4 和定理 5 的证明

设 H_{r} 为一个 r 维 $\mathrm{F_q^2}$ 的子空间，$\beta_1,\beta_2,\cdots,\beta_{\mathrm{r}}$ 为其 $\mathrm{F_2}$ 上的一个基. 再设 $N(H_{\mathrm{r}})=$

$$\{\mathrm{x}=(x,y)\in \mathrm{F_q^2}:\mathrm{Tr}(\mathrm{a}x^{\frac{\mathrm{q}-1}{\rho^{\mathrm{m}}}}+\mathrm{b}y)=1,\ \mathrm{Tr}(\mathrm{x}\bullet\beta_j)=0,1\leq j\leq \mathrm{r}\}$$

.

引理 8　令 H_{r} 为上述一个 r 维 $\mathrm{F_q^2}$ 的子空间. 设

$$B_{H_{\mathrm{r}}}=\sum_{(x,y)\in \mathrm{F_q^2}}\sum_{\beta\in H_{\mathrm{r}}}\chi_1(\beta\bullet(x,y)+\mathrm{a}x^{\frac{\mathrm{q}-1}{\rho^{\mathrm{m}}}}+\mathrm{b}y).$$ 则有

$$\mathrm{d_r}(\mathrm{C_{D(a,b)}})=\mathrm{n}-\frac{\mathrm{q}^2}{2^{\mathrm{r+1}}}+\frac{1}{2^{\mathrm{r+1}}}\min\{B_{H_{\mathrm{r}}}:H_r\in[\mathrm{F_q^2},\ \mathrm{r}]_{\mathrm{p}}\}.$$

证明 由加法特征的正交性质，我们有

$$2^{\mathrm{r+1}}\,|N(H_{\mathrm{r}})|=$$

$$\sum_{\mathrm{x}=(x,y)\in\mathrm{F_q^2}}\Big(\sum_{z\in\mathrm{F_2}}\chi_1\big(z(\mathrm{a}x^{\frac{\mathrm{q}-1}{\rho^{\mathrm{m}}}}+\mathrm{b}y-1)\big)\prod_{i=1}^{\mathrm{r}}\sum_{x_i\in\mathrm{F_2}}\chi_1\big(x_i(\mathrm{x}\bullet\beta_i)\big)\Big)$$

$$=\sum_{\mathrm{x}=(x,y)\in\mathrm{F_q^2}}\Big(\big(1-\chi_1(\mathrm{a}x^{\frac{\mathrm{q}-1}{\rho^{\mathrm{m}}}}+\mathrm{b}y)\big)\sum_{\beta\in H_{\mathrm{r}}}\chi_1(\beta\bullet\mathrm{x})\Big)$$

$$=\mathrm{q}^2-\sum_{\mathrm{x}=(x,y)\in\mathrm{F_q^2}}\sum_{\beta\in H_{\mathrm{r}}}\chi_1(\beta\bullet\mathrm{x}+\mathrm{a}x^{\frac{\mathrm{q}-1}{\rho^{\mathrm{m}}}}+\mathrm{b}y)$$

$$=\mathrm{q}^2-B_{H_{\mathrm{r}}}.$$

我们得到上面的倒数第二个等式，理由是

$$\sum_{\mathrm{x}=(x,y)\in\mathrm{F_q^2}}\sum_{\beta\in H_{\mathrm{r}}}\chi_1(\beta\bullet\mathrm{x})$$

$$=\sum_{\mathrm{x}=(x,y)\in\mathrm{F_q^2}}1+\sum_{\mathrm{x}=(x,y)\in\mathrm{F_q^2}}\sum_{(0,0)\neq\beta\in H_{\mathrm{r}}}\chi_1(\beta\bullet\mathrm{x})$$

$$=\mathrm{q}^2+\sum_{(0,0)\neq\beta\in H_{\mathrm{r}}}\sum_{\mathrm{x}=(x,y)\in\mathrm{F_q^2}}\chi_1(\beta\bullet\mathrm{x})$$

$$=\mathrm{q}^2.$$

因此我们得到$|N(H_{\mathrm{r}})|=\frac{1}{2^{\mathrm{r+1}}}\mathrm{q}^2-\frac{1}{2^{\mathrm{r+1}}}B_{H_{\mathrm{r}}}$. 根据引理 1 及其在文献[27]中的证明可知 $\mathrm{d_r}(\mathrm{C_{D(a,b)}})=\mathrm{n}-\max\{|N(H_{\mathrm{r}})|:H_r\in[\mathrm{F_q^2},\ \mathrm{r}]_{\mathrm{p}}\}$.

因此我们可得该引理中的结论. 证明结束.

下面我们将用引理 1 和引理 8 来解决线性码 $\mathrm{C_{D(a,b)}}$的重量谱.

定理 4 的证明:

(1) 如果$1\le\mathrm{r}\le\frac{1}{2}\phi(\rho^{\mathrm{m}})$，由引理 8 中$B_{H_{\mathrm{r}}}$的定义，我们有

$$B_{H_{\mathrm{r}}}=\sum_{(x,y)\in\mathrm{F_q^2}}\sum_{\beta\in H_{\mathrm{r}}}\chi_1(\beta\bullet(x,y)+\mathrm{a}x^{\frac{\mathrm{q}-1}{\rho^{\mathrm{m}}}}+\mathrm{b}y)$$

$$=\sum_{(x,y)\in\mathrm{F_q^2}}\Big(\sum_{(\beta_1,0)\in H_{\mathrm{r}}}\chi_1(\beta_1x+\mathrm{a}x^{\frac{\mathrm{q}-1}{\rho^{\mathrm{m}}}})+\sum_{\substack{(\beta_1,\beta_2)\in H_{\mathrm{r}}\\ \beta_2\neq0}}\chi_1(\beta_1x+\beta_2y+\mathrm{a}x^{\frac{\mathrm{q}-1}{\rho^{\mathrm{m}}}})\Big)$$

$$=\mathrm{q}\sum_{(\beta_1,0)\in H_{\mathrm{r}}}(1+\mathrm{S}(\mathrm{a},\beta_1)).$$

由引理 4，我们可得$\frac{1}{\mathrm{q}}B_{H_{\mathrm{r}}}=$

$$\sum_{\substack{(\beta_1,0)\in H_{\mathrm{r}}\\ \beta_1\neq0}}\Big(1-\frac{(\sqrt{\mathrm{q}}+1)\mathrm{S(a)}}{\rho^{\mathrm{m}}}+\sqrt{\mathrm{q}}(-1)^{\mathrm{wt}((\mathrm{a}\beta_1^{-\frac{\mathrm{q}-1}{\rho^{\mathrm{m}}}})^{(0)})}\Big)$$

$+1+\frac{(\mathrm{q}-1)\mathrm{S(a)}}{\rho^{\mathrm{m}}}$. 由引理 3，可得 $1-\frac{(\sqrt{\mathrm{q}}+1)\mathrm{S(a)}}{\rho^{\mathrm{m}}}-\sqrt{\mathrm{q}}<0$. 又由引理 5，可知存在一个元素$\beta\in\mathrm{F_q^*}$，使得$\mathrm{wt}((\mathrm{a}\beta^{-\frac{\mathrm{q}-1}{\rho^{\mathrm{m}}}})^{(0)})$为奇数. 回顾我们的设定： 2 是模$\rho^{\mathrm{m}}$一个本原根，同时 $\mathrm{q}=2^{\phi(\rho^{\mathrm{m}})}$. 因此我们有$\mathrm{q}\equiv1(\mathrm{mod}\,\rho^{\mathrm{m}})$及 $\sqrt{\mathrm{q}}\equiv-1(\mathrm{mod}\,\rho^{\mathrm{m}})$. 故对于任意$u\in\mathrm{F}_{\sqrt{\mathrm{q}}}^*$，都有 $(u\beta)^{-\frac{\mathrm{q}-1}{\rho^{\mathrm{m}}}}=\beta^{-\frac{\mathrm{q}-1}{\rho^{\mathrm{m}}}}$. 我们可取一个$\beta\mathrm{F}_{\sqrt{\mathrm{q}}}$的 r 维子空间$\mathrm{L_r}$，构造$H_{\mathrm{r}}=\mathrm{L_r}\times\mathrm{O}$. 对于任意 $(\beta_1,0)\in H_{\mathrm{r}}$，只要$\beta_1\neq0$，都有 $\mathrm{wt}((\mathrm{a}\beta_1^{-\frac{\mathrm{q}-1}{\rho^{\mathrm{m}}}})^{(0)})$为奇数. 此时，$\frac{1}{\mathrm{q}}B_{H_{\mathrm{r}}}$取到它的最小值

$$(2^{\mathrm{r}}-1)\Big(1-\frac{(\sqrt{\mathrm{q}}+1)\mathrm{S(a)}}{\rho^{\mathrm{m}}}-\sqrt{\mathrm{q}}\Big)+1+\frac{(\mathrm{q}-1)\mathrm{S(a)}}{\rho^{\mathrm{m}}}.$$

根据引理 8，当$1\le\mathrm{r}\le\frac{1}{2}\phi(\rho^{\mathrm{m}})$，我们解决了线性码 $\mathrm{C_{D(a,0)}}$的广义汉明重量$\mathrm{d_r}(\mathrm{C_{D(a,0)}})$.

(2) 当 $\frac{1}{2}\phi(\rho^{\mathrm{m}})<\mathrm{r}\le2\phi(\rho^{\mathrm{m}})$ ，则有

$0 \le 2\phi(\rho^m) - r < \frac{3}{2}\phi(\rho^m)$. 由引理 5 或者引理 6 可知，存在一个元素 $(\delta, y) \in D(a,0)$，且满足 $\delta \in F_q$,即有 $Tr(a\delta^{\frac{q-1}{\rho^m}}) = 1$. 对于任意 $u \in F_{\sqrt{q}}^*$，都有 $Tr(a(u\delta)^{\frac{q-1}{\rho^m}}) = Tr(a\delta^{\frac{q-1}{\rho^m}}) = 1$. 因此，$\delta F_{\sqrt{q}} \times F_q \subset D(a,0)$. 选取 $H_{2\phi(\rho^m)-r}$ 为 $\delta F_{\sqrt{q}} \times F_q$ 的一个 $2\phi(\rho^m) - r$ 维子空间. 此时，$|H_{2\phi(\rho^m)-r} \cap D(a,0)| = 2^{2\phi(\rho^m)-r} - 1$. 因此 $\max\{|H \cap D(a,0)| : H \in [F_q, 2\phi(\rho^m) - r]\} = 2^{2\phi(\rho^m)-r} - 1$. 由引理 1，对于 $\frac{1}{2}\phi(\rho^m) < r \le 2\phi(\rho^m)$，$d_r(C_{D(a,0)}) = n - 2^{2\phi(\rho^m)-r} + 1$

$= \frac{q}{2}(q - 1 - \frac{(q-1)S(a)}{\rho^m}) - \frac{1}{2^r}q^2 + 1$. 证明结束.

定理 5 的证明:

(1) 如果 $1 \le r \le \frac{1}{2}\phi(\rho^m)$，由引理 8 中 B_{H_r} 的定义，我们有

$$B_{H_r} = \sum_{(x,y)\in F_q^2}\sum_{(\beta_1,\beta_2)\in H_r}\chi_1(\beta_1 x + \beta_2 y + ax^{\frac{q-1}{\rho^m}} + by)$$

$$= \sum_{(\beta_1,\beta_2)\in H_r}\sum_{x\in F_q}\chi_1(\beta_1 x + ax^{\frac{q-1}{\rho^m}})\sum_{y\in F_q}\chi_1(\beta_2 y + by).$$

令 Prj_2 为 F_q^2 到 F_q 的第二坐标投射：$(x, y) \to y$. 如果 $b \notin Prj_2(H_r)$，对于任意 $(\beta_1, \beta_2) \in H_r$,都有 $\sum_{y\in F_q}\chi_1(\beta_2 y + by) = 0$，因此 $B_{H_r} = 0$.

如果 $b \in Prj_2(H_r)$，则有

$$B_{H_r} = q\sum_{(\beta_1,b)\in H_r}\sum_{x\in F_q}\chi_1(\beta_1 x + ax^{\frac{q-1}{\rho^m}}) = q\sum_{(\beta_1,b)\in H_r}(1 + S(a,\beta_1)).$$

当 $b \in Prj_2(H_r)$ 且 $(0,b) \notin H_r$，由引理 4 可得

$$B_{H_r} = q\sum_{\substack{(\beta_1,b)\in H_r\\ \beta_1\ne 0}}(1 - \frac{(\sqrt{q}+1)S(a)}{\rho^m} + (-1)^{wt((a\beta_1^{\frac{1-q}{\rho^m}})^{(0)})}\sqrt{q}).$$

当 $b \in Prj_2(H_r)$ 且 $(0,b) \in H_r$，由引理 4 可得

$$B_{H_r} = q\sum_{\substack{(\beta_1,b)\in H_r\\ \beta_1\ne 0}}(1 - \frac{(\sqrt{q}+1)S(a)}{\rho^m} + (-1)^{wt((a\beta_1^{\frac{1-q}{\rho^m}})^{(0)})}\sqrt{q}) + q(1 + \frac{(q-1)S(a)}{\rho^m}).$$

由引理 5，存在一个元素 $\beta \in F_q^*$ 满足条件 $wt((a\beta^{-\frac{q-1}{\rho^m}})^{(0)})$ 为奇数. 令 L_{r-1} 为 $\beta F_{\sqrt{q}}$ 的一个 $r-1$ 维子空间. 则对于任意 $u \in F_{\sqrt{q}}^*$，都有 $(u\beta)^{-\frac{q-1}{\rho^m}} = \beta^{-\frac{q-1}{\rho^m}}$. 因此对于 L_{r-1} 中的任意非零元 β_1，均有 $wt((a\beta_1^{-\frac{q-1}{\rho^m}})^{(0)})$ 为奇数. 注意：由引理 3 可知 $1 - \frac{(\sqrt{q}+1)S(a)}{\rho^m} - \sqrt{q} < 0$.

当 $S(a) < 0$，构造 $H_r = L_{r-1} \times bF_2$. 则 $(0,b) \in H_r$. 此时，$\frac{1}{q}B_{H_r}$ 可以取到它的最小值

$$2^{r-1}(1 - \frac{(\sqrt{q}+1)S(a)}{\rho^m} - \sqrt{q}) + \frac{(\sqrt{q}+q)S(a)}{\rho^m} + \sqrt{q}.$$

当 $S(a) > 0$，取 $\xi \in \beta F_{\sqrt{q}} \setminus L_{r-1}$，构造 $H_r = \{(u,0) : u \in L_{r-1}\} \cup \{(\xi + u, b) : u \in L_{r-1}\}$. 易见 H_r 是一个 r 维子空间，而且 $(0,b) \notin H_r$. 此时，$\frac{1}{q}B_{H_r}$ 取到它的最小值 $2^{r-1}(1 - \frac{(\sqrt{q}+1)S(a)}{\rho^m} - \sqrt{q})$. 由引理 8，对于 $1 \le r \le \frac{1}{2}\phi(\rho^m)$，我们解决了广义汉明重量 $d_r(C_{D(a,b)})$.

(3) 当$\frac{1}{2}\phi(\rho^m) < r \le 2\phi(\rho^m)$, 则有 $0 \le 2\phi(\rho^m) - r \le \frac{3}{2}\phi(\rho^m) - 1$. 取一个元素$\delta \in F_q$,满足条件$Tr(a\delta^{\frac{q-1}{\rho^m}}) = 1$. 那么对于任意$u \in F^*_{\sqrt{q}}$，都有$Tr(a(u\delta)^{\frac{q-1}{\rho^m}}) = Tr(a\delta^{\frac{q-1}{\rho^m}}) = 1$.

令$T_b = \{y \in F_q : Tr(by) = 0\}$. 因此, $\delta F_{\sqrt{q}} \times T_b \subset D(a,b)$. 选取$H_{2\phi(\rho^m)-r}$为$\delta F_{\sqrt{q}} \times T_b$的一个$2\phi(\rho^m) - r$维子空间. 此时, $|H_{2\phi(\rho^m)-r} \cap D(a,b)| = 2^{2\phi(\rho^m)-r} - 1$. 因此有

$$\max\{|H \cap D(a,b)| : H \in [F_q, 2\phi(\rho^m) - r]\} = 2^{2\phi(\rho^m)-r} - 1.$$

由引理 1, 对于$\frac{1}{2}\phi(\rho^m) < r \le 2\phi(\rho^m)$,

$$d_r(C_{D(a,b)}) = n - (2^{2\phi(\rho^m)-r} - 1) = \frac{q^2}{2}(1 - \frac{1}{2^{r-1}}) + 1.$$

证明结束.

4 结束语

构造线性码并决定其参数是代数编码理论的重要课题. 近几年来利用定义集法，新的线性码不断被构造出来[2,9,10,12,20-24,35,41,42]. 我们应用一般化了的定义集方法，构造了两类二元线性码，通过指数和理论决定了它们的重量分布，结果显示一类是 3-重另一类为 4-重的低重量线性码. 对于线性码，它的重量谱是较难确定的. 我们综合利用以前得到的一个组合公式和指数和理论完全确定了这两类码的重量谱.

参考文献(References):

[1] M. Bras-Amorós, K. Lee, and A. Vico-Oton. New lower bounds on the generalized Hamming weights of AG codes[J]. IEEE Trans. Inf. Theory，2014，60(10): 5930-5937.

[2] 管玥,施敏加,张欣,伍文婷. 有限域上两类新的2-重量码的构造 [J].电子学报, 2019, 47(3): 714–718.

[3] P. Beelen. A note on the generalized Hamming weights of Reed-Muller codes[J]. Appl. Algebr. Eng. Comm.， 2019， 30：233-242.

[4] J. Cheng and C. Chao. On generalized Hamming weights of binary primitive BCH codes with minimum distance one less than a power of two[J]. IEEE Trans. Inf. Theory，1997，43(1)：294-298.

[5] 陈文德，刘子辉. 码的重量谱•有限射影几何方法[M]. 合肥：中国科学技术大学出版社，2012.

Chen Wende, Liu Zihui. Weight Hierarchy of codes • Finite projective Geometric Approach[M]. Hefei: USTC Press, 2012.

[6] A. R. Calderbank, J. M. Goethals. Three-weight codes and association schemes[J]. Philips J. Res.， 1984， 39：143-152.

[7] A. R. Calderbank, W. M. Kantor. The geometry of two-weight codes[J]. Bull. Lond. Math. Soc.， 1986， 18：97-122.

[8] C. Ding. Linear codes from some 2-designs[J]. IEEE Trans. Inf. Theory，2015，61(6)：3265-3275.

[9] K. Ding, C. Ding. A class of two-weight and three-weight codes and their applications in secret sharing[J]. IEEE Trans. Inf. Theory，2015，61(11)：5835-5842.

[10] K. Ding, C. Ding. Bianry linear codes with three weights[J]. IEEE Commun. Letters，2014，18(11)：1879-1882.

[11] C. Ding, T. Helleseth, T. Klϕve, X. Wang. A generic construction of Cartesian authentication codes[J]. IEEE Trans. Inf. Theory，2007，53(6)：2229-2235.

[12] C. Ding, C. Li, N. Li, Z. Zhou. Three-weight cyclic codes and their weight distributions[J]. Discrete Math.，2016，339(2)：415-427.

[13] T. Helleseth, T. Klϕve, J. Mykkeltveit. The weight distribution of irreducible cyclic codes with block lengths $n_1((q^l-1)/N)$ [J]. Discrete Math.，1977，18(2): 179 - 211.

[14] T. Helleseth, T. Klϕve, and O. Ytrehus. Generalized HammingWeights of Linear Codes[J]. IEEE Trans. Inf. Theory，1992，38(3)：1133-1140.

[15] P. Heijnen and R. Pellikaan. Generalized Hamming weights of q-ary Reed-Muller codes[J]. IEEE Trans. Inf.

Theory，1998，44(1)：181-196.

[16] G. Jian, C. Lin and R. Feng. Two-weight and three-weight linear codes based on Weil sums[J]. Finite Fields Th. App.，2019，57：92-107.

[17] H. Janwa and A. K. Lal. On the generalized Hamming weights of cyclic codes[J]. IEEE Trans. Inf. Theory，1997，43(1)：299-308.

[18] T. Klϕve. The weight distribution of linear codes over GF(q^l) having generator matrix over GF(q) [J]. Discrete Math.，1978，23(2): 159-168.

[19] X. Kong, S. Yang. Complete weight enumerators of a class of linear codes with two or three weights[J]. Discrete Math.，2019，342(11)：3166-3176.

[20] Y. W. Liu and Z. H. Liu. On some classes of codes with a few weights[J]. Adv. Math. Commun.，2018，12(2)：415-428.

[21] H. Liu, Q. Liao. Several classes of linear codes with a few weights from defining sets over F_p+uF_p [J]. Des. Codes Cryptogr.，2017，87(1)：15-29.

[22] R. Lidl, H. Niederreiter. Finite fields[M]. Cambridge University Press, New York，1997.

[23] C. Li, S. Bae, S. Yang. Some results on two-weight and three-weight linear codes[J]. Adv. Math. Commun.，2019，13(1)：195- 211.

[24] C. Li, Q. Yue, F. Fu. A construction of several classes of two-weight and three-weight linear codes[J]. Appl. Algebr. Eng. Comm.，2018，28(1)：1-20.

[25] F. Li. A class of cyclotomic linear codes and their generalized Hamming weights[J]. Appl. Algebr. Eng. Comm.，2018，29：501-511.

[26] F. Li. Weight hierarchy of a class of linear codes relating to non-degenerate quadratic forms[J]. IEEE Trans. Inf. Theory,2020，67(1)：124-129.

[27] F. Li, Xiumei Li. Weight distributions and weight hierarchies of two classes of binary linear codes[J]. Finite Fields Th. App.，2021，73：101865.

[28] Z. Liu, J. Wang. Notes on generalized Hamming weights of some classes of binary codes[J]. Cryptogr. Commun.，2019，12：645-657.

[29] M. Moisio. Explicit evaluation of some exponential sums[J]. Finite Fields Th. App.，2009，15(6)：644-651.

[30] Shi M., Guan Y., Sole P. Two new families of two-weight codes[J]. IEEE Trans. Inf. Theory，2017，63(10)：6240-6246.

[31] Shi M., Liu Y., Sole P. Optimal two weight codes from trace codes over $F_2 + uF_2$[J]. IEEE Communications Letters，2016，20(12)：2346-2349.

[32] Shi M., Wu R., Liu Y., Sole P. Two and three weight codes over $F_p + uF_p$[J]. Cryptogr. Commun.，2017，9(5)：637-646.

[33] Shi M., Liu Y., Sole P. Optimal two weight codes from trace codes over a non-chain ring[J]. Discrete Appl. Math.，2017，219：176-181.

[34] Shi M., Wu R., Qian L., Lin S., Sole P. New Classes of p-ary few weights codes[J]. B. Malays. Math. Sci. So.，2019，42(4)：1393-1412.

[35] C. Tang, C. Xiang, K. Feng. Linear codes with few weights from inhomogeneous quadratic functions[J]. Des. Codes Cryptogr.，2017，83(3)：691-714.

[36] M. A. Tsfasman, S. G. Vlădut. Geometric approach to higher weights[J]. IEEE Trans. Inf. Theory，1995，41(6)：1564-1588.

[37] V. K. Wei. Generalized Hamming weights for linear codes[J]. IEEE Trans. Inf. Theory，1991，37(5)：1412-1418.

[38] M. Xiong, S. Li, and G. Ge. The weight hierarchy of some reducible cyclic codes[J]. IEEE Trans. Inf. Theory，2016，62(7)：4071-4080.

[39] J. Yuan, C. Ding. Secret sharing schemes from three classes of linear codes[J]. IEEE Trans. Inf. Theory，2006，52(1)：206-212.

[40] M. Yang, J. Li, K. Feng and D. Lin. Generalized Hamming weights of irreducible cyclic codes[J]. IEEE Trans. Inf. Theory，2015，61(9)：4905-4913.

[41] S. Yang, Z. A. Yao, C. A. Zhao. The weight distributions of two classes of p-ary cyclic codes with few weights[J]. Finite Fields Th. App.，2017，44：76-91.

[42] Z. Zhou, N. Li, C. Fan and T. Helleseth. Linear codes with two or three weights from quadratic bent functions[J]. Des. Codes Cryptogr.，2016，81(2)：283-295.

【文章到此结束】